Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE CENTERS FOR MEDICARE & MEDICAID SERVICES' IMPLEMENTATION OF SECURITY CONTROLS OVER THE MULTIDIMENSIONAL INSURANCE DATA ANALYTICS SYSTEM NEEDS IMPROVEMENT

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

September 2015
A-06-14-00067

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at http://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Although the Centers for Medicare & Medicaid Services had implemented controls to secure the Multidimensional Insurance Data Analytics System and consumer personally identifiable information, we identified areas for improvement in its information security controls.

This summary report provides an overview of the results of the Office of Inspector General's (OIG) review of the Multidimensional Insurance Data Analytics System (MIDAS). It does not include specific details of the vulnerabilities that we identified because of the sensitive nature of the information. We have provided more detailed information and recommendations to officials responsible for the MIDAS so that they can address the issues we identified. The findings listed in this summary reflect a point in time regarding system security and may have changed since we reviewed these systems.

WHY WE DID THIS REVIEW

Analytics and database systems that are not secured properly create vulnerabilities that could be exploited by unauthorized individuals to compromise the confidentiality of personally identifiable information (PII) or other sensitive data. Data and systems security is a top oversight priority for OIG.

The MIDAS is a central repository for insurance-related data intended to provide reporting and performance metrics to the Department of Health and Human Services for various initiatives mandated by the Patient Protection and Affordable Care Act. The MIDAS collects, generates, and stores a high volume of sensitive consumer information, and it is critical that it be properly secured. Therefore, we performed the audit described in this summary report.

Our objective was to assess whether CMS had implemented information security controls to secure the PII related to the MIDAS and a certain number of its supporting databases.

HOW WE CONDUCTED THIS REVIEW

We focused our audit on information security controls over operations and systems that support MIDAS's database servers. The Centers for Medicare & Medicaid Services (CMS) is responsible for providing guidance and oversight for the MIDAS. Therefore, we reviewed CMS's policies and procedures related to the MIDAS's information security controls. We also examined documentation related to the MIDAS and conducted interviews with CMS representatives who administer the system. We reviewed contractor reports related to vulnerability scans of the MIDAS, determined whether CMS had fully addressed and remediated the vulnerabilities found, and conducted database vulnerability scans. We limited our review of controls to those that were in effect at the time of our audit. We conducted our audit work from August to December 2014.

We conducted the performance audit described here in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and

conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

WHAT WE FOUND AND RECOMMENDED

Although CMS had implemented controls to secure the MIDAS and consumer PII data in the systems and databases we reviewed, we identified areas for improvement in its information security controls. At the time of our fieldwork, CMS:

- had not disabled unnecessary generic accounts[1] in its test environment;
- had not encrypted user sessions;
- had not conducted automated vulnerability assessments that simulate known attacks, which would have revealed vulnerabilities (e.g., password weaknesses and misconfigurations) specific to the application or databases that support the MIDAS; and
- used a shared read-only account for access to the database that contained the PII.

In addition to the information security control vulnerabilities mentioned above, our database vulnerability scans identified 22 high, 62 medium, and 51 low vulnerabilities. We made related recommendations to address the issues we identified.

CMS provided the attached comments on our findings and recommendations.

CMS EFFORTS DURING THE COURSE OF OUR AUDIT

We shared with CMS information about our vulnerability scan findings immediately following the scan and informed CMS about other preliminary findings in advance of issuing our draft report. CMS began remediation efforts before the completion of our fieldwork. In written comments, CMS concurred with all of our recommendations. CMS reported that it remediated all vulnerabilities and addressed all findings we identified before we issued our final report. We have since reviewed the supporting documentation and verified CMS's remediation.

[1] A generic account is an account used for application maintenance or other privileged access that can allow multiple users to access a single account.

APPENDIX: CMS COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

200 Independence Avenue SW
Washington, DC 20201

DATE: MAY - 8 2015

TO: Daniel R. Levinson
Inspector General

FROM: Andrew M. Slavitt
Acting Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: "The Centers for Medicare & Medicaid Services' Implementation of Security Controls Over the Multidimensional Insurance Data Analytics System Needs Improvement" (A-06-14-00067)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on this draft report. The privacy and security of consumers' personally identifiable information (PII) are a top priority for CMS. CMS takes OIG's findings seriously and has implemented all of OIG's recommendations and addressed all of the security vulnerabilities identified in this report.

The privacy and security of consumers' personally identifiable information (PII) are a top priority for CMS. No person or group has maliciously accessed personally identifiable information from HealthCare.gov or its related systems.

The Multidimensional Insurance Data Analytics System (MIDAS) supports HealthCare.gov by acting as a central repository for capturing, aggregating, and analyzing enrollment, plan selection, consumer, and other marketplace data. MIDAS is an internal system accessible only by authorized CMS employees and support personnel. Use of MIDAS must be requested and approved based on appropriate justification before staff or a contractor is granted access. CMS requires MIDAS, like all federal systems that CMS maintains or that are maintained on its behalf, to comply with the Federal Information Security Management Act of 2002 (FISMA). In addition, MIDAS has met the CMS Acceptable Risk Safeguards (ARS) 2.0 security controls identified in Appendix A of the Draft Report.

CMS is focused on continually strengthening our security and privacy controls. In addition to weekly vulnerability assessments of the MIDAS environment, we conduct an annual Security Control Assessment (SCA) that meets Federal and industry standards.

CMS worked with the OIG during the security testing and within a week of the findings being identified, CMS had addressed all the high vulnerabilities identified. CMS had addressed a majority of the remaining findings within 30 days of identification. All of OIG's findings in this

report were addressed by February 2015. In addition, all of the recommendations in this report were fully implemented prior to the draft report being issued.

CMS thanks OIG for their efforts on this issue and looks forward to working with OIG on this and other issues in the future.